B3 cont'

coupled state machine (TCSM) responsive a second set of encryption opcodes,

wherein protocol processing operations are performed by the ALU and encryption operations are performed by the encryption execution unit.

22. (New) The processor of Claim 21, wherein the processor is a microcontroller core (TMC) processor and further comprises:

an instruction fetch stage;

an instruction decode stage to decode an instruction fetched by the instruction fetch stage;

an execution stage to execute a decoded instruction; and

a memory write-back stage to write a result of said execution stage to memory.

a1

23. (New) The processor of Claim 21, further comprise:

one or more internal registers;

a bus operatively connecting the one or more internal registers to both the ALU and the encryption execution unit;

a multiplexer having inputs from both the ALU and the encryption execution unit, the multiplexer outputting a selected input.

24. (New) The processor of Claim 21, wherein the encryption TCSM unit comprises:

a data encryption standard (DES) functional component cooperatively coupled to a sub-key generation functional component.

25. (New) The processor of Claim 24, wherein the DES functional component comprises:

a state machine that executes each round of a DES function.

26. (New) The processor of Claim 24, wherein the sub-key generation functional component comprises:

a state machine that generates a sub-key as needed for each round of the DES function

27. (New) A method for providing encryption functions within a pipelined processor in a network switch, the method comprising the steps of:

associating a first set of opcodes with an ALU internal to the processor;

associating a second set of encryption opcodes with an encryption execution unit internal to the processor having an encryption tightly coupled state machine (TCSM), wherein protocol processing operations are performed by the ALU and encryption operations are performed by the encryption execution unit.

28. (New) The method of Claim 27, further comprise the step of:

providing one or more internal registers;

providing a bus operatively connecting the one or more internal registers to both the ALU and the encryption execution unit;

providing a multiplexer having inputs from both the ALU and the encryption execution unit, the multiplexer outputting a selected input.

29. (New) The method of Claim 27 further comprising the step of:

initializing the encryption TCSM unit in response to a first instruction that defines a form of operation to be performed.

30. (New) The method of Claim 29, wherein the step of initializing comprises the steps of:

decoding a first portion of the first instruction to initialize the DES functional component; and

decoding a second portion of the first instruction to initialize the sub-key generation functional component.

31. (New) The method of Claim 27, further comprising the steps of:

executing a second instruction including an encryption opcode that specifies loading an initial key from a memory into the sub-key generation functional component of the TCSM unit.

32. (New) The method of Claim 27, further comprising the steps of:

performing a DES function in response to execution of a third instruction having a field containing an encryption opcode that specifies loading plaintext and initialing the DES operations;

33. (New) A computer readable media, comprising: said computer readable media containing instructions for execution in a processor for the practice of the method of claim 10 or claim 27.

34. (New) Electromagnetic signals propagating on a computer network, comprising: said electromagnetic signals carrying instructions for execution on a processor for the practice of the method of claim 10 or claim 27.